

# Cryptosystems Using Automorphisms of Finitely Generated Free Groups

Anja I. S. Moldenhauer and Gerhard Rosenberger

Fachbereich Mathematik, Universität Hamburg,  
Bundesstrasse 55, 20146 Hamburg, Germany  
anja.moldenhauer@uni-hamburg.de, gerhard.rosenberger@math.uni-hamburg.de

**Abstract.** This paper introduces a newly developed private key cryptosystem and a public key cryptosystem. In the first one, each letter is encrypted with a different key. Therefore, it is a kind of a one-time pad. The second one is inspired by the ElGamal cryptosystem. Both presented cryptosystems are based on automorphisms of free groups. Given a free group  $F$  of finite rank, the automorphism group  $\text{Aut}(F)$  can be generated by Nielsen transformations, which are the basis of a linear technique to study free groups and general infinite groups. Therefore Nielsen transformations are introduced.

**Keywords:** private key cryptosystem, public key cryptosystem, free group  $F$  of finite rank, automorphism group  $\text{Aut}(F)$ , Nielsen transformations, Whitehead-Automorphisms.

*Dedicated to Gabriele Kern-Isberner on the occasion of her 60th birthday<sup>1</sup>.*

## 1 Introduction

The topic of this paper is established in the area of mathematical cryptology, more precisely in group based cryptology. We refer to the books [1], [7] and [13] for the interested reader. The books [1] and [7] can also be used for a first access to the wide area of cryptology.

We introduce two cryptosystems, the first one is a private key cryptosystem (one-time pad) and the second one is a public key cryptosystem. We require that the reader is familiar with the general concept of these types of protocols. In cryptology it is common to call the two parties who want to communicate privately with each other Alice and Bob.

Throughout the paper let  $F$  always be a free group  $F = \langle X \mid \quad \rangle$  of finite rank. Both cryptosystems are based on free groups  $F$  of finite rank and automorphisms of  $F$ . It is known that the group of all automorphisms of  $F$ ,  $\text{Aut}(F)$ , can be generated by Nielsen transformations (see [3]).

We first review some basic definitions concerning regular Nielsen transformations and Nielsen reduced sets and we give additional information which is

<sup>1</sup> This article appeared 2016 in College Publications Tributes Volume 29: **Computational Models of Rationality** *Essays Dedicated to Gabriele Kern-Isberner on the Occasion of Her 60th Birthday*.

also important for the understanding of the paper.

Both cryptosystems use automorphisms of a free group  $F$  of finite rank. Thus, a random choice of these automorphisms is practical. An approach for this random choice using the Whitehead-Automorphisms is given. Therefore, the Whitehead-Automorphisms are reviewed. Note, that the Whitehead-Automorphisms generate the Nielsen transformations and vice versa, but the use of the Whitehead-Automorphisms is more practical if a random choice of automorphisms is required.

After this, a private key cryptosystem using Nielsen transformations and Nielsen reduced sets is introduced. An example and a security analysis for this private key cryptosystem is given. Finally we explain a public key cryptosystem which is inspired by the ElGamal cryptosystem, from which we describe two variations and give an example.

The new cryptographic protocols are in part in the dissertation [12] of A. Moldenhauer under her supervisor G. Rosenberger at the University of Hamburg.

## 2 Preliminaries for Automorphisms of Free Groups

We now review some basic definitions concerning regular Nielsen transformations and Nielsen reduced sets and we give additional information which will be used later on (see also [3], [9] or [10]).

Let  $F$  be a free group on the free generating set  $X := \{x_1, x_2, \dots, x_q\}$  and let  $U := \{u_1, u_2, \dots, u_t\} \subset F$ ,  $q, t \geq 2$ . A **freely reduced word** in  $X$  is a word in which the symbols  $x_i^\epsilon$ ,  $x_i^{-\epsilon}$ , for  $\epsilon = \pm 1$  and  $i = 1, 2, \dots, q$ , do not occur consecutively. We call  $q$  the **rank of  $F$** . The free generating set  $X$  is also called a **basis** of  $F$ . The elements  $u_i$  are freely reduced words with letters in  $X^{\pm 1} := X \cup X^{-1}$ , with  $X^{-1} := \{x_1^{-1}, x_2^{-1}, \dots, x_q^{-1}\}$ .

### Definition 1.

*An **elementary Nielsen transformation** on*

$U = \{u_1, u_2, \dots, u_t\} \subset F$  *is one of the following transformations*

- (T1) *replace some  $u_i$  by  $u_i^{-1}$ ;*
- (T2) *replace some  $u_i$  by  $u_i u_j$  where  $j \neq i$ ;*
- (T3) *delete some  $u_i$  where  $u_i = 1$ .*

*In all three cases the  $u_k$  for  $k \neq i$  are not changed. A (finite) product of elementary Nielsen transformations is called a **Nielsen transformation**. A Nielsen transformation is called **regular** if it is a finite product of the transformations (T1) and (T2), otherwise it is called **singular**. The regular Nielsen transformations generate a group. The set  $U$  is called **Nielsen-equivalent** to the set  $V$ , if there is a regular Nielsen transformation from  $U$  to  $V$ . Nielsen-equivalent sets  $U$  and  $V$  generate the same group, that is,  $\langle U \rangle = \langle V \rangle$ .*

Now, we agree on some notations. We write  $(T1)_i$  if we replace  $u_i$  by  $u_i^{-1}$  and we write  $(T2)_{i,j}$  if we replace  $u_i$  by  $u_i u_j$ . If we want to apply the same Nielsen transformation (T2) consecutively  $t$ -times we write  $[(T2)_{i,j}]^t$  and hence replace  $u_i$  by  $u_i u_j^t$ . In all cases the  $u_k$  for  $k \neq i$  are not changed.

**Definition 2.**

A finite set  $U$  in  $F$  is called **Nielsen reduced**, if for any three elements  $v_1, v_2, v_3$  from  $U^{\pm 1}$  the following conditions hold:

- (N0)  $v_1 \neq 1$ ;
- (N1)  $v_1 v_2 \neq 1$  implies  $|v_1 v_2| \geq |v_1|, |v_2|$ ;
- (N2)  $v_1 v_2 \neq 1$  and  $v_2 v_3 \neq 1$  implies  $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$ .

Here  $|v|$  denotes the **free length** of  $v \in F$ , that is, the number of letters from  $X^{\pm 1}$  in the freely reduced word  $v$ .

*Remark 1.* We say that any word  $w$  with finitely many letters from  $X^{\pm 1}$  has **length**  $L$  if the number of letters occurring is  $L$ . The length of a word  $w$  is greater than or equal to the free length of the word  $w$ . For freely reduced words the length and the free length are equal. If a word  $w$  is not freely reduced then the length is greater than the free length of  $w$ .

**Proposition 1.** [3, Theorem 2.3] or [9, Proposition 2.2]

If  $U = \{u_1, u_2, \dots, u_m\}$  is finite, then  $U$  can be carried by a Nielsen transformation into some  $V$  such that  $V$  is Nielsen reduced. We have  $\text{rank}(\langle V \rangle) \leq m$ .

**Proposition 2.** [10, Corollary 3.1]

Let  $H$  be a finitely generated subgroup of the free group  $F$  on the free generating set  $X$ . Let  $U = \{u_1, u_2, \dots, u_t\}$ ,  $u_i$  words in  $X$ , be a Nielsen reduced set. Then, out of all systems of generators for  $H$ , the set  $U$  has the shortest total  $x$ -length, that is  $\sum_{i=1}^t |u_i|$ .

*Remark 2.* If  $F_V$  is a finitely generated subgroup of  $F = \langle X \mid \rangle$ , with free generating set  $V = \{v_1, v_2, \dots, v_N\}$ ,  $v_i$  words in  $X$ , then there exist only finitely many Nielsen reduced sets  $U_i = \{u_{i1}, u_{i2}, \dots, u_{iN}\}$ ,  $i = 1, 2, \dots, \ell$ , to  $V$ , which are Nielsen-equivalent. With the help of a lexicographical order  $<_{lex}$  (see for instance [3, Proof of Satz 2.3]) the smallest set  $U_s$ , in the set of all Nielsen reduced sets  $U_{Nred}^V := \{U_1, U_2, \dots, U_\ell\}$  to  $V$ , can be uniquely marked. With the use of regular Nielsen transformations it is possible to obtain this marked set  $U_s$  starting from any arbitrary set in  $U_{Nred}^V$ .

**Proposition 3.** [3, Korollar 2.10]

Let  $F$  be the free group of rank  $q$ . Then, the group of all automorphisms of  $F$ ,  $\text{Aut}(F)$ , is generated by the elementary Nielsen transformations (T1) and (T2).

More precisely: Each automorphism of  $F$  is describable as a regular Nielsen transformation between two bases of  $F$ , and, each regular Nielsen transformation between two bases of  $F$  defines an automorphism of  $F$ .

*Remark 3.* In [16] an algorithm, using elementary Nielsen transformations, is presented which, given a finite set  $S$  of  $m$  words of a free group, returns a set  $S'$  of Nielsen reduced words such that  $\langle S \rangle = \langle S' \rangle$ ; the algorithm runs in  $\mathcal{O}(\ell^2 m^2)$  time, where  $\ell$  is the maximum length of a word in  $S$ .

**Theorem 1.** [3, Satz 2.6]

Let  $U$  be Nielsen reduced, then  $\langle U \rangle$  is free on  $U$ .

For the next lemma we need some notations. Let  $w \neq 1$  be a freely reduced word in  $X$ . The initial segment  $s$  of  $w$  which is “a little more than half” of  $w$  (that is,  $\frac{1}{2}|w| < |s| \leq \frac{1}{2}|w| + 1$ ) is called the **major initial segment** of  $w$ . The **minor initial segment** of  $w$  is that initial segment  $s'$  which is “a little less than half” of  $w$  (that is,  $\frac{1}{2}|w| - 1 \leq |s'| < \frac{1}{2}|w|$ ). Similarly, **major** and **minor terminal segments** are defined.

If the free length of the word  $w$  is even, we call the initial segment  $s$  of  $w$ , with  $|s| = \frac{1}{2}|w|$  the **left half** of  $w$ . Analogously, we call the terminal segment  $s'$  of  $w$  with  $|s'| = \frac{1}{2}|w|$  the **right half** of  $w$ .

Let  $\{w_1, w_2, \dots, w_n\}$  be a set of freely reduced words in  $X$ , which are not the identity. An initial segment of a  $w$ -symbol (that is, of either  $w_i$  or  $w_i^{-1}$ , which are different  $w$ -symbols) is called **isolated** if it does not occur as an initial segment of any other  $w$ -symbol. Similarly, a terminal segment is isolated if it is a terminal segment of a unique  $w$ -symbol.

**Lemma 1.** [10, Lemma 3.1]

Let  $M := \{w_1, w_2, \dots, w_m\}$  be a set of freely reduced words in  $X$  with  $w_j \neq 1$ ,  $1 \leq j \leq m$ . Then  $M$  is Nielsen reduced if and only if the following conditions are satisfied:

1. Both the major initial and major terminal segments of each  $w_i \in M$  are isolated.
2. For each  $w_i \in M$  of even free length, either its left half or its right half is isolated.

**Definition 3.**

Let  $F$  be a free group of rank  $q$  and let  $G$  be a free subgroup of  $F$  with rank  $m$ . An element  $g \in G$  is called a **primitive element** of  $G$ , if a basis  $U$  of  $G$  with  $g \in U$  exists.

**Proposition 4.** [14]

The number of primitive elements of free length  $k$  of the free group

$F_2 = \langle x_1, x_2 \mid \rangle$  (and therefore, in any group  $F_q = \langle x_1, x_2, \dots, x_q \mid \rangle$ ,  $q \geq 2$ ) is:

1. more than  $\frac{8}{3\sqrt{3}} \cdot (\sqrt{3})^k$  if  $k$  is odd;
2. more than  $\frac{4}{3} \cdot (\sqrt{3})^k$  if  $k$  is even.

**Theorem 2.** [2]

If  $P(q, k)$  is the number of primitive elements of free length  $k$  of the free group

$F_q = \langle x_1, x_2, \dots, x_q \mid \rangle$ ,  $q \geq 3$ , then for some constants  $c_1, c_2$ , we have

$$c_1 \cdot (2q - 3)^k \leq P(q, k) \leq c_2 \cdot (2q - 2)^k.$$

**Definition 4.** [15]

A subgroup  $H$  of  $F$  is called **characteristic** in  $F$  if  $\varphi(H) = H$  for every automorphism  $\varphi$  of  $F$ .

For  $n \in \mathbb{N}$  let  $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$  be the ring of integers modulo  $n$ . The corresponding residue class in  $\mathbb{Z}_n$  for an integer  $\beta$  is denoted by  $\overline{\beta}$  (see also [1]).

**Definition 5.** [1]

Let  $n \in \mathbb{N}$  and  $\bar{\beta}, \bar{\gamma} \in \mathbb{Z}_n$ . A bijective mapping  $h : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  given by  $x \mapsto \bar{\beta}x + \bar{\gamma}$  is called a **linear congruence generator**.

**Theorem 3.** [1] (Maximal period length for  $n = 2^m$ ,  $m \in \mathbb{N}$ )

Let  $n \in \mathbb{N}$ , with  $n = 2^m$ ,  $m \geq 1$  and let  $\beta, \gamma \in \mathbb{Z}$  such that  $h : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ , with  $x \mapsto \bar{\beta}x + \bar{\gamma}$ , is a linear congruence generator. Further let  $\alpha \in \{0, 1, \dots, n-1\}$  be given and  $x_1 = \bar{\alpha}$ ,  $x_2 = h(x_1)$ ,  $x_3 = h(x_2)$ ,  $\dots$

Then the sequence  $x_1, x_2, x_3, \dots$  is periodic with maximal periodic length  $n = 2^m$  if and only if the following holds:

1.  $\beta$  is odd.
2. If  $m \geq 2$  then  $\beta \equiv 1 \pmod{4}$ .
3.  $\gamma$  is odd.

**Theorem 4.** [8]

Let  $F$  be a free group with countable number of generators  $x_1, x_2, \dots$ . Corresponding to  $x_j$  define

$$M_j = \begin{pmatrix} -r_j & -1 + r_j^2 \\ 1 & -r_j \end{pmatrix}$$

with  $r_j \in \mathbb{Q}$  and

$$\begin{aligned} r_{j+1} - r_j &\geq 3 \\ r_1 &\geq 2. \end{aligned}$$

Then  $G^*$  generated by  $\{M_1, M_2, \dots\}$  is isomorphic to  $F$ .

### 3 The Random Choice of the Automorphisms of $Aut(F)$

Let  $F = \langle X \mid \quad \rangle$  be the free group on the free generating set  $X$  with  $|X| = q$ . The cryptosystems we develop are based on automorphisms of  $F$ . These automorphisms should be chosen randomly. It is known, see Proposition 3, that the Nielsen transformations generate the automorphism group  $Aut(F)$ . For a realization of a random choice procedure the Whitehead-Automorphisms will be used.

A fixed set of randomly chosen automorphisms is part of the key space for the private key cryptosystem.

**Definition 6.** *Whitehead-Automorphisms:*

1. Invert the letter  $a$  and leave all other letters invariant:

$$i_a(b) = \begin{cases} a^{-1} & \text{for } a = b \\ b & \text{for } b \in X \setminus \{a\}. \end{cases}$$

There are  $q$  **Whitehead-Automorphisms** of this type.

2. Let  $a \in X$  and  $L, R, M$  be three pairwise disjoint subsets of  $X$ , with  $a \in M$ . Then the tuple  $(a, L, R, M)$  defines a **Whitehead-Automorphisms**  $W_{(a,L,R,M)}$  as follows

$$W_{(a,L,R,M)}(b) = \begin{cases} ab & \text{for } b \in L \\ ba^{-1} & \text{for } b \in R \\ aba^{-1} & \text{for } b \in M \\ b & \text{for } b \in X \setminus (L \cup M \cup R). \end{cases}$$

There are  $q \cdot 4^{q-1}$  automorphisms of this type.

Note, that  $W_{(a,L,R,M)}^{-1} = i_a \circ W_{(a,L,R,M)} \circ i_a$ .

With this definition it is clear how the Whitehead-Automorphisms can be generated as a product of regular Nielsen transformations. Conversely, the Whitehead-Automorphisms generate the group of the Nielsen transformations and therefore also the automorphism group  $Aut(F)$  (see also [4]). With the Whitehead-Automorphisms it is simple to realize a random choice of automorphisms. We now give an approach for this choice.

#### An approach for choosing randomly automorphisms of $Aut(F)$ :

Let  $X = \{x_1, x_2, \dots, x_q\}$  be the free generating set for the free group  $F$ .

1. First of all it should be decided in which order an automorphism  $f_i$  is generated by automorphisms of type  $i_a$  and  $W_{(a,L,R,M)}$ . For this purpose an automorphism of type  $i_a$  is identified with a zero and  $W_{(a,L,R,M)}$  with a one. A sequence of zeros and ones is randomly generated. This sequence is translated to randomly chosen Whitehead-Automorphisms and hence presents an automorphism  $f_i \in Aut(F)$ . This translation is as follows:
  - 2.1. For a zero in the sequence we generate  $i_a$  randomly: choose a random number  $z$ , with  $1 \leq z \leq q$ ; hence an element  $a \in X$  must be chosen to declare the automorphism. Then it is  $a := x_z$  and hence  $x_z$  is replaced by  $x_z^{-1}$  and all other letters are invariant.
  - 2.2. For a one in the sequence we generate  $W_{(a,L,R,M)}$  randomly: choose a random number  $z$ , with  $1 \leq z \leq q$ . Hence it is  $a := x_z$ . Moreover it is  $a \in M$ . After this the disjoint sets  $L, R, M \subset X$  are chosen randomly. One possible approach is the following:
    - (a) Choose random numbers  $z_1, z_2$  and  $z_3$  with

$$\begin{aligned} 0 &\leq z_1 \leq q-1, \\ 0 &\leq z_2 \leq q-1-z_1, \\ 0 &\leq z_3 \leq q-1-z_1-z_2. \end{aligned}$$

If we are in the situation of  $z_1 = z_2 = z_3 = 0$  we get the identity  $id_X$ . If this case arises a random number  $\tilde{z}$  from the set  $\{1, 2, \dots, q\} \setminus \{z\}$  is chosen and hence the element  $x_{\tilde{z}}$  is assigned randomly to one of the sets  $L, R$  or  $M$ ; therefore the identity is avoided.

It is

$$|L| = z_1, \quad |R| = z_2, \quad |M| = z_3 + 1.$$

- (b) Choose  $z_1$  pairwise different random numbers  $\{r_1, r_2, \dots, r_{z_1}\}$  of the set  $\{1, 2, \dots, q\} \setminus \{z\}$ . Then  $L$  is the set

$$L = \{x_{r_1}, x_{r_2}, \dots, x_{r_{z_1}}\}.$$

- (c) Choose  $z_2$  pairwise different random numbers  $\{p_1, p_2, \dots, p_{z_2}\}$  of the set  $\{1, 2, \dots, q\} \setminus (\{z\} \cup \{r_1, r_2, \dots, r_{z_1}\})$ . Then  $R$  is the set

$$R = \{x_{p_1}, x_{p_2}, \dots, x_{p_{z_2}}\}.$$

- (d) Choose  $z_3$  pairwise different random numbers  $\{t_1, t_2, \dots, t_{z_3}\}$  of the set  $\{1, 2, \dots, q\} \setminus (\{z\} \cup \{r_1, r_2, \dots, r_{z_1}\} \cup \{p_1, p_2, \dots, p_{z_2}\})$ . Then  $M$  is the set

$$M = \{x_{t_1}, x_{t_2}, \dots, x_{t_{z_3}}\} \cup \{a\}.$$

*Remark 4.* If Alice and Bob use Whitehead-Automorphisms to generate automorphisms on a free group with free generating set  $X$  they should take care, that there are no sequences of the form

1.  $i_a \circ i_a = id_X$ ,
  2.  $W_{(a,L,R,M)} \circ i_a \circ \underbrace{W_{(a,L,R,M)}}_{=W_{(a,L,R,M)}^{-1}} \circ i_a = id_X$  or
- $$\underbrace{i_a \circ W_{(a,L,R,M)}}_{=W_{(a,L,R,M)}^{-1}} \circ i_a \circ W_{(a,L,R,M)} = id_X,$$

for the automorphism  $f_j$ . They also should not use Whitehead-Automorphisms sequences for  $f_j$ , which cancel each other and so be vacuous for the encryption.

## 4 Private Key Cryptosystem Based on Automorphisms of Free Groups $F$

Before Alice and Bob are able to communicate with each other, they have to make some arrangements.

### Public Parameters

They first agree on the public parameters.

1. A free group  $F$  with free generating set  $X = \{x_1, x_2, \dots, x_q\}$ , with  $q \geq 2$ .
2. A plaintext alphabet  $A = \{a_1, a_2, \dots, a_N\}$ , with  $N \geq 2$ .
3. A subset  $\mathcal{F}_{aut} := \{f_1, f_2, \dots, f_{2^{128}}\} \subset Aut(F)$  of automorphisms of  $F$  is chosen. It is  $f_i : F \rightarrow F$  and the  $f_i, i = 1, 2, \dots, 2^{128}$ , pairwise different, are generated with the help of 0-1-sequences (of different length) and random numbers as described in Section 3. The set  $\mathcal{F}_{aut}$  is part of the key space.

4. They agree on a linear congruence generator  $h : \mathbb{Z}_{2^{128}} \rightarrow \mathbb{Z}_{2^{128}}$  with a maximal period length (see Definition 5 and Theorem 3).

*Remark 5.* If the set  $\mathcal{F}_{aut}$  and the linear congruence generator  $h$  are public Alice and Bob are able to change the automorphisms and the generator publicly without a private meeting. The set  $\mathcal{F}_{aut}$  should be large enough to make a brute force search ineffective.

Another variation could be, that Alice and Bob choose the number of elements in the starting set  $\mathcal{F}_{aut}$  smaller than  $2^{128}$ , say for example  $2^{10}$ . These starting automorphism set  $\mathcal{F}_{aut}$  should be chosen privately by Alice and Bob as their set of seeds and should not be made public. Then Alice and Bob can extend publicly the starting set  $\mathcal{F}_{aut}$  to the set  $\mathcal{F}_{aut_1}$  of automorphisms such that  $\mathcal{F}_{aut_1}$  contains, say for example,  $2^{32}$  automorphisms. The number of all elements in  $\mathcal{F}_{aut_1}$  should make a brute force attack inefficient. The linear congruence generator stays analogously, just the domain and codomain must be adapted to, say for example,  $\mathbb{Z}_{2^{32}}$ . Because of Theorem 3 Alice and Bob get at all times a linear congruence generator with maximal periodic length.

### Private Parameters

Now they agree on the private parameters.

1. A free subgroup  $F_U$  of  $F$  with rank  $N$  and the free generating set  $U = \{u_1, u_2, \dots, u_N\}$  is chosen where  $U$  is a minimal Nielsen reduced set (with respect to a lexicographical order) and the  $u_i$  freely reduced words in  $X$ . Such systems  $U$  are easily to construct using Theorem 1 and Lemma 1 (see also [3] and [9]). It is  $\mathcal{U}_{Nred}$  the set of all minimal Nielsen reduced sets with  $N$  elements in  $F$ , which is part of the key space.
2. They use a one to one correspondence

$$\begin{aligned} A &\rightarrow U \\ a_j &\mapsto u_j \quad \text{for } j = 1, \dots, N. \end{aligned}$$

3. Alice and Bob agree on an automorphism  $f_{\bar{\alpha}} \in \mathcal{F}_{Aut}$ , hence  $\alpha$  is the common secret starting point  $\alpha \in \{0, 1, \dots, 2^{128} - 1\}$ , with  $x_1 = \bar{\alpha} \in \mathbb{Z}_{2^{128}}$ , for the linear congruence generator. With this  $\alpha$  they are able to generate the sequence of automorphisms of the set  $\mathcal{F}_{aut}$ , which they use for encryption and decryption, respectively.

**The key space:** The set  $\mathcal{U}_{Nred}$  of all minimal (with respect to a lexicographical order) Nielsen reduced subsets of  $F$  with  $N$  elements. The set  $\mathcal{F}_{Aut}$  of  $2^{128}$  randomly chosen automorphisms of  $F$ .

### Protocol

Now we explain the protocol and look carefully at the steps for Alice and Bob.

**Public knowledge:**  $F = \langle X \mid \rangle$ ,  $X = \{x_1, x_2, \dots, x_q\}$  with  $q \geq 2$ ; plaintext alphabet  $A = \{a_1, a_2, \dots, a_N\}$  with  $N \geq 2$ ; the set  $\mathcal{F}_{Aut}$ ; a linear



congruence generator  $h$ .

**Encryption and Decryption Procedure:**

1. Alice and Bob agree privately on a set  $U \in \mathcal{U}_{Nred}$  and an automorphism  $f_{\overline{\alpha}} \in \mathcal{F}_{Aut}$ . They also know the one to one correspondence between  $U$  and  $A$ .
2. Alice wants to transmit the message

$$S = s_1 s_2 \cdots s_z, \quad z \geq 1,$$

with  $s_i \in A$  to Bob.

- 2.1. Alice generates with the linear congruence generator  $h$  and the knowledge of  $f_{\overline{\alpha}}$  the  $z$  automorphisms  $f_{x_1}, f_{x_2}, \dots, f_{x_z}$ , which she needs for encryption. It is  $x_1 = \overline{\alpha}, x_2 = h(x_1), \dots, x_z = h(x_{z-1})$ .
- 2.2. The encryption is as follows

$$\text{if } s_i = a_t \quad \text{then } s_i \mapsto c_i := f_{x_i}(a_t), \quad 1 \leq i \leq z, \quad 1 \leq t \leq N.$$

Recall that the one to one correspondence  $A \rightarrow U$  with  $a_j \mapsto u_j$ , for  $j = 1, 2, \dots, N$ , holds. The ciphertext

$$\begin{aligned} C &= f_{x_1}(s_1) f_{x_2}(s_2) \cdots f_{x_z}(s_z) \\ &= c_1 c_2 \cdots c_z \end{aligned}$$

is sent to Bob. We call  $c_j$  the ciphertext units. We do no cancellations between  $c_i$  and  $c_{i+1}$ , for  $1 \leq i \leq z-1$ .

3. Bob gets the ciphertext

$$C = c_1 c_2 \cdots c_z,$$

and the information that he has to use  $z$  automorphisms of  $F$  from the set  $\mathcal{F}_{Aut}$  for decryption. He has now two possibilities for decryption.

- 3.1.a. With the knowledge of  $f_{\overline{\alpha}}$ , the linear congruence generator  $h$  and the number  $z$ , he computes for each automorphism  $f_{x_i}$ ,  $i = 1, 2, \dots, z$ , the inverse automorphism  $f_{x_i}^{-1}$ .
- 3.1.b. With the knowledge of  $f_{\overline{\alpha}}$ , the set  $U = \{u_1, u_2, \dots, u_N\}$ , the linear congruence generator  $h$  and the number  $z$ , he computes for each automorphism  $f_{x_i}$ ,  $i = 1, 2, \dots, z$ , the set

$$U_{f_{x_i}} = \{f_{x_i}(u_1), f_{x_i}(u_2), \dots, f_{x_i}(u_N)\}.$$

Hence, with the one to one correspondence between  $U$  and  $A$ , he gets a one to one correspondence between the letters in the alphabet  $A$  and the words of the ciphertext depending on the automorphisms  $f_{x_i}$ . This is shown in Table 1.

**Table 1.** Plaintext alphabet  $A = \{a_1, a_2, \dots, a_N\}$  corresponded to ciphertext alphabet  $U_{f_{x_i}}$  depending on the automorphisms  $f_{x_i}$ 

	$U_{f_{x_1}}$	$U_{f_{x_2}}$	$\dots$	$U_{f_{x_z}}$
$a_1$	$f_{x_1}(u_1)$	$f_{x_2}(u_1)$	$\dots$	$f_{x_z}(u_1)$
$a_2$	$f_{x_1}(u_2)$	$f_{x_2}(u_2)$	$\dots$	$f_{x_z}(u_2)$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$a_N$	$f_{x_1}(u_N)$	$f_{x_2}(u_N)$	$\dots$	$f_{x_z}(u_N)$

3.2. With the knowledge of the Table 1 or the inverse automorphisms  $f_{x_i}^{-1}$ , respectively, the decryption is as follows

$$\text{if } c_i = f_{x_i}(u_t) \quad \text{then } c_i \mapsto s_i := f_{x_i}^{-1}(c_i) = u_t, \quad 1 \leq i \leq z, \quad 1 \leq t \leq N.$$

He generates the plaintext message

$$\begin{aligned} S &= f_{x_1}^{-1}(c_1) f_{x_2}^{-1}(c_2) \dots f_{x_z}^{-1}(c_z) \\ &= s_1 s_2 \dots s_z, \end{aligned}$$

with  $s_i \in A$ , from Alice.

*Remark 6.* The cryptosystem is a polyalphabetic system. A word  $u_i \in U$ , and hence a letter  $a_i \in A$ , is encrypted differently at different places in the plaintext.

*Example 1.* This example was executed with the help of the computer program GAP and the package “FGA<sup>2</sup>”.

First Alice and Bob agree on the **public parameters**.

1. Let  $F$  be the free group on the free generating set  $X = \{a, b, c, d\}$ .
2. Let  $\tilde{A} := \{a_1, a_2, \dots, a_{12}\} = \{A, E, I, O, U, T, M, L, K, Y, B, N\}$  be the plaintext alphabet.
3. A set  $\mathcal{F}_{Aut}$  is determined. In this example we give the automorphisms, which Alice and Bob use for encryption and decryption, respectively, just at the moment when they are needed.
4. The linear congruence generator with maximal periodic length is

$$\begin{aligned} h : \mathbb{Z}_{2^{128}} &\rightarrow \mathbb{Z}_{2^{128}} \\ x &\mapsto \overline{5}x + \overline{3}. \end{aligned}$$

<sup>2</sup> Free Group Algorithms, a GAP4 Package by Christian Sievers, TU Braunschweig.

The **private parameters** for this example are:

1. The free group  $F_{\tilde{U}}$  of  $F$  with the free generating set

$$\begin{aligned}\tilde{U} = & \{u_1, u_2, \dots, u_{12}\} \\ = & \{ba^2, cd, d^2c^{-2}, a^{-1}b, a^4b^{-1}, b^3a^{-2}, bc^3, bc^{-1}bab^{-1}, \\ & c^2ba, c^2dab^{-1}, a^{-1}d^3c^{-1}, a^2db^2d^{-1}\}.\end{aligned}$$

It is known, that  $a_i \mapsto u_i$ ,  $i = 1, 2, \dots, 12$ , for  $u_i \in \tilde{U}$  and  $a_i \in \tilde{A}$ . The set  $\tilde{U}$  is a Nielsen reduced set and the group  $F_{\tilde{U}}$  has rank 12. Alice and Bob agree on the starting automorphism  $f_{\overline{93}}$ , hence it is  $x_1 = \overline{\alpha} = \overline{93}$ .

We look at the **encryption and decryption procedure** for Alice and Bob.

2. With the above agreements **Alice** is able to encrypt her message

$$S = \text{I LIKE BOB.}$$

Her message is of length 8. She generates the ciphertext as follows:

- 2.1. She first determines, with the help of the linear congruence generator  $h$ , the automorphisms  $f_{x_i}$ ,  $i = 1, 2, \dots, 8$ , which she needs for encryption. It is

$$\begin{aligned}x_1 = \overline{\alpha} &= \overline{93}, & x_2 = h(x_1) &= \overline{468}, & x_3 = h(x_2) &= \overline{2343}, \\ x_4 = h(x_3) &= \overline{11718}, & x_5 = h(x_4) &= \overline{58593}, & x_6 = h(x_5) &= \overline{292968}, \\ x_7 = h(x_6) &= \overline{1464843}, & x_8 = h(x_7) &= \overline{7324218}.\end{aligned}$$

The automorphisms are described with the help of regular Nielsen transformations, it is

$$f_{x_1} = (N1)_3(N2)_{1.4}(N2)_{4.3}(N2)_{2.3}(N1)_3(N2)_{1.4}(N2)_{3.1},$$

$$\begin{aligned}f_{x_1} : F &\rightarrow F \\ a &\mapsto ad^2c^{-1}, \quad b \mapsto bc^{-1}, \quad c \mapsto cad^2c^{-1}, \quad d \mapsto dc^{-1};\end{aligned}$$

$$f_{x_2} = (N2)_{1.4}(N1)_2(N2)_{2.4}(N2)_{3.1}(N1)_2(N1)_1(N2)_{1.3}[(N2)_{4.3}]^2(N1)_3,$$

$$\begin{aligned}f_{x_2} : F &\rightarrow F \\ a &\mapsto d^{-1}a^{-1}cad, \quad b \mapsto d^{-1}b, \quad c \mapsto d^{-1}a^{-1}c^{-1}, \quad d \mapsto d(cad)^2;\end{aligned}$$

$$f_{x_3} = (N1)_2(N2)_{4.2}(N1)_4(N2)_{2.4}(N1)_2(N2)_{4.2}(N1)_3(N2)_{2.1}(N2)_{3.2}[(N2)_{1.4}]^3(N1)_2(N2)_{4.2},$$

$$\begin{aligned}f_{x_3} : F &\rightarrow F \\ a &\mapsto ab^3, \quad b \mapsto a^{-1}d^{-1}, \quad c \mapsto c^{-1}da, \quad d \mapsto ba^{-1}d^{-1};\end{aligned}$$

$$f_{x_4} = [(N2)_{3.1}]^2(N1)_2[(N2)_{2.1}]^3(N2)_{2.4}(N2)_{4.2}(N2)_{1.3},$$

$$\begin{aligned}f_{x_4} : F &\rightarrow F \\ a &\mapsto aca^2, \quad b \mapsto b^{-1}a^3d, \quad c \mapsto ca^2, \quad d \mapsto db^{-1}a^3d;\end{aligned}$$

$$f_{x_5} = (N2)_{1.2}(N1)_3(N1)_1[(N2)_{4.3}]^2(N2)_{1.2}(N1)_2(N1)_3(N2)_{2.4}(N2)_{3.1},$$

$$f_{x_5} : F \rightarrow F$$

$$a \mapsto b^{-1}a^{-1}b, \quad b \mapsto b^{-1}dc^{-2}, \quad c \mapsto cb^{-1}a^{-1}b, \quad d \mapsto dc^{-2};$$

$$f_{x_6} = (N1)_1(N2)_{2.3}(N2)_{3.1}(N1)_2(N2)_{1.2}(N2)_{4.2},$$

$$f_{x_6} : F \rightarrow F$$

$$a \mapsto a^{-1}c^{-1}b^{-1}, \quad b \mapsto c^{-1}b^{-1}, \quad c \mapsto ca^{-1}, \quad d \mapsto dc^{-1}b^{-1};$$

$$f_{x_7} = [(N2)_{2.1}]^3(N1)_3[(N2)_{4.3}]^3(N1)_1(N2)_{1.2}(N1)_2(N2)_{2.4}(N2)_{3.1},$$

$$f_{x_7} : F \rightarrow F$$

$$a \mapsto a^{-1}ba^3, \quad b \mapsto a^{-3}b^{-1}dc^{-3}, \quad c \mapsto c^{-1}a^{-1}ba^3, \quad d \mapsto dc^{-3};$$

$$f_{x_8} = (N2)_{1.4}(N1)_2(N1)_3(N2)_{2.1}[(N2)_{3.4}]^2(N1)_4(N1)_1(N1)_3(N2)_{4.2},$$

$$f_{x_8} : F \rightarrow F$$

$$a \mapsto d^{-1}a^{-1}, \quad b \mapsto b^{-1}ad, \quad c \mapsto d^{-2}c, \quad d \mapsto d^{-1}b^{-1}ad.$$

Note, that the regular Nielsen transformations are applied from the left to the right.

2.2 The ciphertext is now

$$\begin{aligned} C &= f_{x_1}(\mathbf{I})f_{x_2}(\mathbf{L})f_{x_3}(\mathbf{I})f_{x_4}(\mathbf{K})f_{x_5}(\mathbf{E})f_{x_6}(\mathbf{B})f_{x_7}(\mathbf{O})f_{x_8}(\mathbf{B}) \\ &= f_{x_1}(d^2c^{-2})f_{x_2}(bc^{-1}bab^{-1})f_{x_3}(d^2c^{-2})f_{x_4}(c^2ba)f_{x_5}(cd)f_{x_6}(a^{-1}d^3c^{-1}) \\ &\quad f_{x_7}(a^{-1}b)f_{x_8}(a^{-1}d^3c^{-1}) \\ &= dc^{-1}d^{-1}a^{-1}d^{-2}a^{-1}c^{-1} \wr d^{-1}bcabd^{-1}a^{-1}cadb^{-1}d \wr \\ &\quad (ba^{-1}d^{-1})^2(a^{-1}d^{-1}c)^2 \wr (ca^2)^2b^{-1}a^3daca^2 \wr cb^{-1}a^{-1}bdc^{-2} \wr \\ &\quad bca(dc^{-1}b^{-1})^3ac^{-1} \wr a^{-1}(a^{-2}b^{-1})^2dc^{-3} \wr (ab^{-1})^3adc^{-1}d^2 \\ &= c_1c_2c_3c_4c_5c_6c_7c_8. \end{aligned}$$

The symbol “ $\wr$ ” marks the end of a ciphertext unit  $c_i$ .

3. **Bob** gets the ciphertext

$$\begin{aligned} C &= dc^{-1}d^{-1}a^{-1}d^{-2}a^{-1}c^{-1} \wr d^{-1}bcabd^{-1}a^{-1}cadb^{-1}d \wr \\ &\quad (ba^{-1}d^{-1})^2(a^{-1}d^{-1}c)^2 \wr (ca^2)^2b^{-1}a^3daca^2 \wr cb^{-1}a^{-1}bdc^{-2} \wr \\ &\quad bca(dc^{-1}b^{-1})^3ac^{-1} \wr a^{-1}(a^{-2}b^{-1})^2dc^{-3} \wr (ab^{-1})^3adc^{-1}d^2 \end{aligned}$$

from Alice. Now he knows, that he needs eight automorphisms for decryption.

3.1. Bob knows the set  $U$ , the linear congruence generator  $h$  and the starting seed automorphism  $f_{\overline{93}}$ . For decryption he uses tables (analogously to Table 1).

Now, he is able to compute for each automorphism  $f_{x_i}$  the set  $U_{f_{x_i}}$ ,  $i = 1, 2, \dots, 8$ , and to generate the tables Table 2, Table 3, Table 4 and Table 5.

**Table 2.** Correspondence: plaintext alphabet to ciphertext alphabet I

	$U_{f_{x_1}}$	$U_{f_{x_2}}$
$A$	$b(c^{-1}ad^2)^2c^{-1}$	$d^{-1}bd^{-1}a^{-1}c^2ad$
$E$	$cad(dc^{-1})^2$	$d^{-1}a^{-1}c^{-1}(dca)^2d$
$I$	$dc^{-1}d^{-1}a^{-1}d^{-2}a^{-1}c^{-1}$	$((dca)^2d)^2cadcad$
$O$	$cd^{-2}a^{-1}bc^{-1}$	$d^{-1}a^{-1}c^{-1}ab$
$U$	$(ad^2c^{-1})^3ad^2b^{-1}$	$d^{-1}a^{-1}c^4adb^{-1}d$
$T$	$(bc^{-1})^2bd^{-2}a^{-1}cd^{-2}a^{-1}$	$(d^{-1}b)^3d^{-1}a^{-1}c^{-2}ad$
$M$	$b(ad^2)^3c^{-1}$	$d^{-1}b(d^{-1}a^{-1}c^{-1})^3$
$L$	$bd^{-2}a^{-1}c^{-1}bc^{-1}ad^2b^{-1}$	$d^{-1}bcabd^{-1}a^{-1}cadb^{-1}d$
$K$	$c(ad^2)^2c^{-1}bc^{-1}ad^2c^{-1}$	$(d^{-1}a^{-1}c^{-1})^2d^{-1}bd^{-1}a^{-1}cad$
$Y$	$c(ad^2)^2c^{-1}dc^{-1}ad^2b^{-1}$	$(d^{-1}a^{-1}c^{-1})^2dcadc^2adb^{-1}d$
$B$	$cd^{-2}a^{-1}(dc^{-1})^2d^{-1}a^{-1}c^{-1}$	$d^{-1}a^{-1}c^{-1}(ad^2cadc)^3adcad$
$N$	$(ad^2c^{-1})^2d(c^{-1}b)^2d^{-1}$	$d^{-1}a^{-1}c^2ad(dca)^2bd^{-1}b(d^{-1}a^{-1}c^{-1})^2d^{-1}$

**Table 3.** Correspondence: plaintext alphabet to ciphertext alphabet II

	$U_{f_{x_3}}$	$U_{f_{x_4}}$
$A$	$a^{-1}d^{-1}(ab^3)^2$	$b^{-1}a^3d(aca^2)^2$
$E$	$c^{-1}daba^{-1}d^{-1}$	$ca^2db^{-1}a^3d$
$I$	$(ba^{-1}d^{-1})^2(a^{-1}d^{-1}c)^2$	$(db^{-1}a^3d)^2a^{-2}c^{-1}a^{-2}c^{-1}$
$O$	$b^{-3}a^{-2}d^{-1}$	$a^{-2}c^{-1}a^{-1}b^{-1}a^3d$
$U$	$(ab^3)^4da$	$(aca^2)^4d^{-1}a^{-3}b$
$T$	$(a^{-1}d^{-1})^3(b^{-3}a^{-1})^2$	$(b^{-1}a^3d)^3a^{-2}c^{-1}a^{-3}c^{-1}a^{-1}$
$M$	$a^{-1}d^{-1}(c^{-1}da)^3$	$b^{-1}a^3d(ca^2)^3$
$L$	$(a^{-1}d^{-1})^2ca^{-1}d^{-1}ab^3da$	$b^{-1}a^3da^{-2}c^{-1}b^{-1}a^3daca^2d^{-1}a^{-3}b$
$K$	$c^{-1}dac^{-1}ab^3$	$(ca^2)^2b^{-1}a^3daca^2$
$Y$	$(c^{-1}da)^2ba^{-1}d^{-1}ab^3da$	$(ca^2)^2db^{-1}a^3daca^2d^{-1}a^{-3}b$
$B$	$b^{-3}a^{-1}(ba^{-1}d^{-1})^3a^{-1}d^{-1}c$	$a^{-2}c^{-1}a^{-1}(db^{-1}a^3d)^3a^{-2}c^{-1}$
$N$	$(ab^3)^2b(a^{-1}d^{-1})^2b^{-1}$	$aca^3c(a^2db^{-1}a)^2a^2$

**Table 4.** Correspondence: plaintext alphabet to ciphertext alphabet III

	$U_{f_{x_5}}$	$U_{f_{x_6}}$
A	$b^{-1}dc^{-2}b^{-1}a^{-2}b$	$(c^{-1}b^{-1}a^{-1})^2c^{-1}b^{-1}$
E	$cb^{-1}a^{-1}bdc^{-2}$	$ca^{-1}dc^{-1}b^{-1}$
I	$dc^{-2}dc^{-1}(c^{-1}b^{-1}ab)^2c^{-1}$	$(dc^{-1}b^{-1})^2ac^{-1}ac^{-1}$
O	$b^{-1}adc^{-2}$	$bca c^{-1}b^{-1}$
U	$b^{-1}a^{-4}bc^2d^{-1}b$	$(a^{-1}c^{-1}b^{-1})^3a^{-1}$
T	$(b^{-1}dc^{-2})^3b^{-1}a^2b$	$(c^{-1}b^{-1})^2abca$
M	$b^{-1}dc^{-1}(b^{-1}a^{-1}bc)^2b^{-1}a^{-1}b$	$c^{-1}b^{-1}(ca^{-1})^3$
L	$b^{-1}dc^{-2}b^{-1}abc^{-1}b^{-1}dc^{-2}b^{-1}a^{-1}bc^2d^{-1}b$	$c^{-1}b^{-1}ac^{-2}b^{-1}a^{-1}$
K	$cb^{-1}a^{-1}bcb^{-1}a^{-1}dc^{-2}b^{-1}a^{-1}b$	$ca^{-1}c(a^{-1}c^{-1}b^{-1})^2$
Y	$(cb^{-1}a^{-1}b)^2dc^{-2}b^{-1}a^{-1}bc^2d^{-1}b$	$(ca^{-1})^2dc^{-1}b^{-1}a^{-1}$
B	$b^{-1}ab(dc^{-2})^3b^{-1}abc^{-1}$	$bca(dc^{-1}b^{-1})^3ac^{-1}$
N	$b^{-1}a^{-2}b(dc^{-2}b^{-1})^2$	$(a^{-1}c^{-1}b^{-1})^2d(c^{-1}b^{-1})^2d^{-1}$

**Table 5.** Correspondence: plaintext alphabet to ciphertext alphabet IV

	$U_{f_{x_7}}$	$U_{f_{x_8}}$
A	$a^{-3}b^{-1}dc^{-3}a^{-1}(ba^2)^2a$	$b^{-1}d^{-1}a^{-1}$
E	$c^{-1}a^{-1}ba^3dc^{-3}$	$d^{-2}cd^{-1}b^{-1}ad$
I	$dc^{-3}dc^{-3}(a^{-3}b^{-1}ac)^2$	$d^{-1}(b^{-1}a)^2(dc^{-1}d)^2d$
O	$a^{-1}(a^{-2}b^{-1})^2dc^{-3}$	$adb^{-1}ad$
U	$a^{-1}(ba^2)^4ac^3d^{-1}ba^3$	$(d^{-1}a^{-1})^5b$
T	$(a^{-3}b^{-1}dc^{-3})^3a^{-1}(a^{-2}b^{-1})^2a$	$(b^{-1}ad)^3adad$
M	$a^{-3}b^{-1}dc^{-3}(c^{-1}a^{-1}ba^3)^3$	$b^{-1}a(d^{-1}cd^{-1})^2d^{-1}c$
L	$a^{-3}b^{-1}dc^{-3}a^{-3}b^{-1}aca^{-3}b^{-1}dc^{-3}a^{-1}ba^3c^3d^{-1}ba^3$	$b^{-1}adc^{-1}d^2b^{-1}d^{-1}a^{-1}b$
K	$c^{-1}a^{-1}ba^3c^{-1}a^{-1}dc^{-3}a^{-1}ba^3$	$(d^{-2}c)^2b^{-1}$
Y	$(c^{-1}a^{-1}ba^3)^2dc^{-3}a^{-1}ba^3c^3d^{-1}ba^3$	$(d^{-2}c)^2d^{-1}b^{-1}d^{-1}a^{-1}b$
B	$a^{-3}b^{-1}a(dc^{-3})^3a^{-3}b^{-1}ac$	$(ab^{-1})^3adc^{-1}d^2$
N	$a^{-1}(ba^2)^2a(dc^{-3}a^{-3}b^{-1})^2$	$(d^{-1}a^{-1})^2d^{-1}(b^{-1}ad)^2d$

3.2. With these tables he is able to generate the plaintext from Alice, it is

$$\begin{aligned}
S &= f_{x_1}^{-1} (dc^{-1}d^{-1}a^{-1}d^{-2}a^{-1}c^{-1}) f_{x_2}^{-1} (d^{-1}bcabd^{-1}a^{-1}cadb^{-1}d) \\
&\quad f_{x_3}^{-1} ((ba^{-1}d^{-1})^2(a^{-1}d^{-1}c)^2) f_{x_4}^{-1} ((ca^2)^2b^{-1}a^3daca^2) \\
&\quad f_{x_5}^{-1} (cb^{-1}a^{-1}bdc^{-2}) f_{x_6}^{-1} (bca(dc^{-1}b^{-1})^3ac^{-1}) \\
&\quad f_{x_7}^{-1} (a^{-1}(a^{-2}b^{-1})^2dc^{-3}) f_{x_8}^{-1} ((ab^{-1})^3adc^{-1}d^2) \\
&= \text{I LIKE BOB.}
\end{aligned}$$

### Security

This private key cryptosystem is secure against chosen plaintext attacks and chosen ciphertext attacks. In a chosen plaintext attack, an attacker, Eve, chooses an arbitrary plaintext of her choice and gets the corresponding ciphertext. In a chosen ciphertext attack Eve sees ciphertexts and gets to some of these ciphertexts the corresponding plaintexts (see also [1]).

An eavesdropper, Eve, intercepts the ciphertext

$$C = c_1c_2 \cdots c_z,$$

with  $c_i = f_{x_i}(u_j)$  for some  $1 \leq j \leq N$ . If Alice and Bob choose non characteristic subgroups, then it is likely that  $c_j \notin F_U$  for some  $1 \leq j \leq z$ . Hence the ciphertext units give no hint for the subgroup  $F_U$ . Eve knows  $L = \sum_{k=1}^z |c_k|$ , the length of  $C$ , because Alice and Bob are doing no cancellations between  $c_i$  and  $c_{i+1}$ , for  $1 \leq i \leq z-1$ .

To break the system Eve needs to know the set  $U$ . For this it is likely that she assumes that the ball  $B(F, L)$  in the Cayleygraph for  $F$  contains a basis for  $F_U$ . With this assumption she searches for primitive elements for  $F_U$  in the ball  $B(F, L)$ ,  $|y| \leq L$ ,  $y \in F$ . In fact she needs to find  $N$  primitive elements for  $F_U$  in  $B(F, L)$  (these would be primitive elements for  $F_U$  in a ball  $B(F_U, L)$  for some Nielsen reduced basis for  $F_U$ ). From Proposition 4 and Theorem 2 it is known that the number of primitive elements grows exponentially with the free length of the elements. Eve chooses sets  $M_i := \{m_{i_1}, m_{i_2}, \dots, m_{i_K}\}$  with  $K \geq N$  and elements  $m_{i_j}$  in  $B(F, L)$  and with Nielsen transformations she constructs the corresponding Nielsen reduced sets  $M'_i$ . If  $|M'_i| = N$  then  $M'_i$  is a candidate for  $U$ .

The number  $N$  is a constant in the cryptosystem, hence it takes  $\mathcal{O}(\lambda^2)$  time, with  $\lambda := \max\{|m_{j_\ell}| \mid \ell = 1, 2, \dots, K\} \leq L$ , to get the set  $M'_j$  from  $M_j$  with the algorithm [16] (see Remark 3).

The main security certification depends on the fact, that for a single subset of  $K$  elements Eve finds a Nielsen reduced set in polynomial running time (more precisely in quadratic time) but she has to test all possible subsets of  $K$  elements for which she needs exponential running time.

The security certification can be improved by the next two improvements.

First, Alice and Bob choose in addition an explicit presentation of the ciphertext units  $c_i$  as matrices in  $SL(2, \mathbb{Q})$ . So, they agree on a faithful representation

$$\begin{aligned}\varphi : F &\rightarrow SL(2, \mathbb{Q}) \\ x_i &\mapsto M_i,\end{aligned}$$

of  $F$  into  $SL(2, \mathbb{Q})$  (see Theorem 4). The group  $G = \varphi(F)$  is isomorphic to  $F$  under the mapping  $x_i \mapsto M_i$ , for  $i = 1, \dots, q$ . The ciphertext is now

$$\begin{aligned}C' &= \varphi(c_1)\varphi(c_2)\cdots\varphi(c_z) \\ &= W_1W_2\cdots W_z,\end{aligned}$$

a sequence of matrices  $W_j \in SL(2, \mathbb{Q})$ . The encryption is realizable with a table (as Table 1) if the representation  $\varphi$  is applied to the elements in the table. Therefore Bob gets a table with matrices and hence an assignment from the matrices to the plaintext alphabet depending on the automorphisms  $f_{x_i}$ .

Here the additional security certification is, that there is no algorithm known to solve the membership problem (see for instance [10]) for subgroups of  $SL(2, \mathbb{Q})$  which are not subgroups in  $SL(2, \mathbb{Z})$ . B. Eick, M. Kirschner and C. Leedham-Green presented in the paper [5] a practical algorithm to solve the constructive membership problem for discrete free subgroups of rank 2 of  $SL(2, \mathbb{R})$ . For example, the subgroup  $SL(2, \mathbb{Z})$  of  $SL(2, \mathbb{R})$  is discrete. But they also mention, that it is an open problem to solve the membership problem for arbitrary subgroups of  $SL(2, \mathbb{R})$  with rank  $m \geq 2$ . Alice and Bob work with subgroups of rank  $N \geq 2$ . Hence there is in general no algorithm known for Eve to solve the membership problem, in particular there is always no such algorithm known for  $N \geq 3$ .

*Example 2.* In this example<sup>3</sup> Alice and Bob agree additionally to Example 1 on a faithful representation. With Theorem 4 they generate the matrices

$$X_1 := \begin{pmatrix} -\frac{7}{2} & \frac{45}{4} \\ 1 & -\frac{7}{2} \end{pmatrix}, \quad X_2 := \begin{pmatrix} -\frac{15}{2} & \frac{221}{4} \\ 1 & -\frac{15}{2} \end{pmatrix} \quad \text{and} \quad X_3 := \begin{pmatrix} -\frac{23}{2} & \frac{525}{4} \\ 1 & -\frac{23}{2} \end{pmatrix}.$$

These matrices form a basis for a free group  $G$  of rank 3. Alice and Bob generate a subgroup  $G_1$  of  $G$  with rank 4. The free generating set for  $G_1$  is  $\{X_1X_2, X_3X_1^2, X_2X_3X_2, X_1^{-1}X_2\}$ . They choose the faithful representation

$$\begin{aligned}\varphi : F &\rightarrow SL(2, \mathbb{Q}) \\ a &\mapsto X_1X_2 = \begin{pmatrix} \frac{75}{2} & -\frac{1111}{4} \\ -11 & \frac{163}{2} \end{pmatrix}, & b &\mapsto X_3X_1^2 = \begin{pmatrix} -1189 & 3990 \\ 104 & -349 \end{pmatrix}, \\ c &\mapsto X_2X_3X_2 = \begin{pmatrix} -2681 & 19966 \\ 360 & -2681 \end{pmatrix}, & d &\mapsto X_1^{-1}X_2 = \begin{pmatrix} 15 & -109 \\ 4 & -29 \end{pmatrix}.\end{aligned}$$

---

<sup>3</sup> We realized this example with the computer programs Classic Worksheet Maple 16 and GAP. In GAP we used the package ‘‘FGA’’ (Free Group Algorithms, a GAP4 Package by Christian Sievers, TU Braunschweig).



The ciphertext is now

$$\begin{aligned}
C' = & \varphi(dc^{-1}d^{-1}a^{-1}d^{-2}a^{-1}c^{-1}) \varphi(d^{-1}bcabd^{-1}a^{-1}cadb^{-1}d) \\
& \varphi((ba^{-1}d^{-1})^2(a^{-1}d^{-1}c)^2) \varphi((ca^2)^2b^{-1}a^3daca^2) \varphi(cb^{-1}a^{-1}bdc^{-2}) \\
& \varphi(bca(dc^{-1}b^{-1})^3ac^{-1}) \varphi(a^{-1}(a^{-2}b^{-1})^2dc^{-3}) \varphi((ab^{-1})^3adc^{-1}d^2) \\
= & \left( \frac{-429743093559909}{2} \frac{-6400784021410159}{4} \right) \\
& \left( \frac{-3240070331754423030683243991}{2} \frac{-932216979117085}{2} \right) \\
& \left( \frac{-3240070331754423030683243991}{2} \frac{47007695458416827592369656315}{4} \right) \\
& \left( \frac{-223326322203710575272321977}{2} \frac{3240070327830150751386194361}{2} \right) \\
& \left( \frac{-6899014060703475554169965}{2} \frac{102756972145191520348785607}{4} \right) \\
& \left( \frac{301722468685102729969483}{2} \frac{-4493988131847945704997109}{2} \right) \\
& \left( \frac{-397074726172421275253684843812134445}{2} \frac{5883318761059670223751985896578473377}{4} \right) \\
& \left( \frac{26659253089426526822952736194350493}{2} \frac{-395000924306510751052288425218790757}{2} \right) \\
& \left( \frac{46475888407425825}{2} \frac{692232489736400389}{2} \right) \\
& \left( \frac{-3120351373297111}{2} \frac{-46475896943687759}{2} \right) \\
& \left( \frac{-37154085868492177463035768197599}{2} \frac{-553374013794643763898030444104547}{4} \right) \\
& \left( \frac{1624906569753714749910956723073}{2} \frac{24201404758781402065719318991873}{2} \right) \\
& \left( \frac{-3418963163764785449276501363}{2} \frac{-50923553357916815212095363641}{4} \right) \\
& \left( \frac{-230751369629481141540301125}{2} \frac{-3436913216344813651054341083}{2} \right) \\
& \left( \frac{2739747352948144349387}{2} \frac{-39628644296581967709615}{4} \right) \\
& \left( \frac{-402070084312200114547}{2} \frac{5815679440792026855107}{2} \right).
\end{aligned}$$

Instead of a sequence of words in  $F$  Alice sends to Bob a sequence of eight matrices in  $\text{SL}(2, \mathbb{Q})$ .

For the second improvement Alice and Bob use instead of a presentation of the ciphertext in  $\text{SL}(2, \mathbb{Q})$  a presentation of the ciphertext in a free group in  $\text{GL}(2, k)$  with  $k := \mathbb{Z}[y_1, y_2, \dots, y_w]$ , the ring of polynomials in variables  $y_1, y_2, \dots, y_w$ . With the help of a homomorphism  $\epsilon^* : \text{GL}(2, k) \rightarrow \text{GL}(2, \mathbb{Z})$  and the knowledge of an algorithm to write each element in the modular group  $\text{PSL}(2, \mathbb{Z})$ , the group of  $2 \times 2$  projective integral matrices of determinant 1, in terms of  $s$  and  $t$  they can reconstruct the message. Here,

$$s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and  $\text{PSL}(2, \mathbb{Z}) = \langle s, t \mid s^2 = (st)^3 = 1 \rangle$ .

Every finitely generated free group is faithfully represented by a subgroup of the modular group  $\text{PSL}(2, \mathbb{Z})$ . Especially, the two matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$$

generate a free group of rank two, and this free group certainly contains finitely generated free groups.

This improvement is very similar to the version in [1]. Here, the security certification depends in addition on the unsolvability of Hilbert's Tenth Problem. Y. Matiyasevich proved in [11] that there is no general algorithm which determines whether or not an integral polynomial in any number of variables has a zero.

## 5 Public Key Cryptosystem Based on Automorphisms of Free Groups $F$

Now we describe a public key cryptosystem for Alice and Bob which is inspired by the ElGamal cryptosystem (see [6] or [13, Section 1.3]), based on discrete logarithms, that is:

1. Alice and Bob agree on a finite cyclic group  $G$  and a generating element  $g \in G$ .
2. Alice picks a random natural number  $a$  and publishes the element  $c := g^a$ .
3. Bob, who wants to transmit a message  $m \in G$  to Alice, picks a random natural number  $b$  and sends the two elements  $m \cdot c^b$  and  $g^b$ , to Alice. Note that  $c^b = g^{ab}$ .
4. Alice recovers  $m = (m \cdot c^b) \cdot ((g^b)^a)^{-1}$ .

Let  $X = \{x_1, x_2, \dots, x_N\}$ ,  $N \geq 2$ , be the free generating set of the free group  $F = \langle X \mid \rangle$ . It is  $X^{\pm 1} = X \cup X^{-1}$ . The message is an element  $m \in S^*$ , the set of all freely reduced words with letters in  $X^{\pm 1}$ . Public are the free group  $F$ , its free generating set  $X$  and an element  $a \in S^*$ . The automorphism  $f$  should be chosen randomly, for example as it is described in Section 3.

The public key cryptosystem is now as follows:

**Public parameters:** The group  $F = \langle X \mid \rangle$ , a freely reduced word  $a \neq 1$  in the free group  $F$  and an automorphism  $f : F \rightarrow F$  of infinite order.

### Encryption and Decryption Procedure:

1. Alice chooses privately a natural number  $n$  and publishes the element  $f^n(a) =: c \in S^*$ .
2. Bob picks privately a random  $t \in \mathbb{N}$  and his message  $m \in S^*$ . He calculates the freely reduced elements

$$m \cdot f^t(c) =: c_1 \in S^* \quad \text{and} \quad f^t(a) =: c_2 \in S^*.$$

He sends the ciphertext  $(c_1, c_2) \in S^* \times S^*$  to Alice.

3. Alice calculates

$$\begin{aligned} c_1 \cdot f^n(c_2)^{-1} &= m \cdot f^t(c) \cdot f^n(c_2)^{-1} \\ &= m \cdot f^t(f^n(a)) \cdot (f^n(f^t(a)))^{-1} \\ &= m \cdot f^{t+n}(a) \cdot (f^{n+t}(a))^{-1} \\ &= m, \end{aligned}$$

and gets the message  $m$ .

*Remark 7.* A possible attacker, Eve, can see the elements  $c, c_1, c_2 \in S^*$ . She does not know the free length of  $m$  and the cancellations between  $m$  and  $f^t(c)$  in  $c_1$ . It could be possible that  $m$  is completely canceled by the first letters of

$f^t(c)$ . Hence she cannot determine  $m$  from the given  $c_1$ . Eve just sees words,  $f^t(a)$  and  $f^n(a)$ , in the free generating set  $X$  from which it is unlikely to realize the exponents  $n$  and  $t$ , that is, the private keys from Alice and Bob, respectively. The security certification is based on the Diffie-Hellman-Problem.

*Remark 8.* We give some ideas to enhance the security, they can also be combined:

1. The element  $a \in S^*$  could be taken as a common private secret between Alice and Bob. They could use for example the Anshel-Anshel-Goldfeld key exchange protocol (see [13]) to agree on the element  $a$ .
2. Alice and Bob agree on a faithful representation from  $F$  into the special linear group of all  $2 \times 2$  matrices with entries in  $\mathbb{Q}$ , that is,  $g : F \rightarrow \text{SL}(2, \mathbb{Q})$ . Now  $m \in S^*$  and Bob sends  $g(m) \cdot g(f^t(c)) =: c_1 \in \text{SL}(2, \mathbb{Q})$  instead of  $m \cdot f^t(c) =: c_1 \in S^*$ ;  $c$  and  $c_2$  remain the same. Therefore, Alice calculates  $c_1 \cdot (g(f^n(c_2)))^{-1} = g(m)$  and hence the message  $m = g^{-1}(g(m)) \in S^*$ . This variation in addition extends the security certification to the membership problem in the matrix group  $\text{SL}(2, \mathbb{Q})$  (see [5]).

*Example 3.*

This example<sup>4</sup> is a very small one and it is just given for illustration purposes. Bob wants to send a message to Alice.

The **public parameters** are the free group  $F = \langle x_1, x_2, x_3 \mid \rangle$  of rank 3, the freely reduced word  $a \in F$ , with  $a := x_1^2 x_2 x_3^{-2} x_2$  and the automorphism  $f : F \rightarrow F$ , which is given, for this example, by regular Nielsen transformations:  $f = [(N2)_{1,2}]^2 (N2)_{3,2} (N1)_3 (N2)_{2,3}$ , that is,

$$x_1 \mapsto x_1 x_2^2, \quad x_2 \mapsto x_3^{-1}, \quad x_3 \mapsto x_2^{-1} x_3^{-1}.$$

1. Alice's private key is  $n = 7$ . Thus, she gets the automorphism

$$\begin{aligned} f^7 : F &\rightarrow F \\ x_1 &\mapsto x_1 x_2^2 x_3^{-1} x_2 (x_2 x_3)^2 (x_3 x_2 x_3^2 x_2)^2 x_3 x_2 \\ x_2 &\mapsto x_2^{-1} ((x_3^{-1} x_2^{-1} x_3^{-1})^2 x_2^{-1} x_3^{-1})^2 x_3^{-1} x_2^{-1} x_3^{-2} \\ x_3 &\mapsto (((x_2^{-1} x_3^{-1})^2 x_3^{-1})^2 x_2^{-1} x_3^{-2})^2 x_2^{-1} (x_3^{-1} x_2^{-1} x_3^{-1})^2 x_3^{-1}. \end{aligned}$$

Her public key is

$$\begin{aligned} c := f^7(a) &= (x_1 x_2^2 x_3^{-1} x_2 (x_2 x_3)^2 (x_3 x_2 x_3^2 x_2)^2 x_3 x_2)^2 (x_3^2 x_2)^2 \\ &\quad ((x_3 x_2 x_3)^2 x_2 x_3)^2 x_3 x_2 x_3^2 x_2 x_3^{-1}. \end{aligned}$$

2. Bob privately picks the ephemeral key  $t = 5$  and gets the automorphism

$$\begin{aligned} f^5 : F &\rightarrow F \\ x_1 &\mapsto x_1 x_2^2 x_3^{-1} x_2^2 x_3 (x_3 x_2)^2 \\ x_2 &\mapsto x_2^{-1} (x_3^{-1} x_2^{-1} x_3^{-1})^2 x_3^{-1} \\ x_3 &\mapsto ((x_2^{-1} x_3^{-1})^2 x_3^{-1})^2 x_2^{-1} x_3^{-2}. \end{aligned}$$

---

<sup>4</sup> We used the computer program GAP and the package "FGA" (Free Group Algorithms, a GAP4 Package by Christian Sievers, TU Braunschweig).

His message for Alice is  $m = x_3^{-2}x_2^2x_3x_1^2x_2^{-1}x_1^{-1}$ . He calculates

$$\begin{aligned} c_1 &= m \cdot f^5(c) \\ &= x_3^{-2}x_2^2x_3x_1^2(x_2x_3^{-1})^2((x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-2}x_2^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-1})^2x_3^{-1}x_2^{-1} \\ &\quad (((x_3^{-1}x_2^{-1}x_3^{-1})^2x_2^{-1}x_3^{-1})^2x_3^{-1}x_2^{-1}x_3^{-1}x_2^{-1}x_3^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-1} \\ &\quad x_2^{-1}x_3^{-1})^2((x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-2}x_2^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-1})^2x_3^{-1}x_1x_2^2x_3^{-1}x_2(x_3^{-1} \\ &\quad (((x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-2}x_2^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-1})^2x_3^{-1}x_2^{-1})^3(x_3^{-1}x_2^{-1}x_3^{-1})^2 \\ &\quad x_2^{-1}x_3^{-1}((x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-2}x_2^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-1})^2x_2^{-1})^3x_3^{-1} \\ &\quad ((x_3^{-1}x_2^{-1}x_3^{-2}x_2^{-1})^2x_3^{-2}x_2^{-1})^2(x_3^{-1}x_2^{-1}x_3^{-1})^2x_2^{-1}x_3^{-1}x_2 \end{aligned}$$

and

$$c_2 := f^5(a) = (x_1x_2^2x_3^{-1}x_2^2x_3(x_3x_2)^2)^2x_3^2x_2(x_3x_2x_3)^2x_3x_2x_3^{-1}.$$

The ciphertext for Alice is the tuple  $(c_1, c_2)$ .

### 3. Alice first computes

$$\begin{aligned} (f^7(c_2))^{-1} &= x_2^{-1}((((x_3x_2)^2x_3)^2x_3x_2x_3)^2x_3x_2(x_3x_2x_3)^2)^2x_3x_2 \\ &\quad ((x_3x_2x_3)^2x_2x_3)^2x_3x_2x_3)^2(x_3x_2((x_3x_2x_3)^2x_2x_3)^2x_3x_2x_3x_2x_3)^2 \\ &\quad (x_3x_2x_3^2x_2)^2x_3)^2x_2((((x_3^2x_2)^2x_3x_2)^2x_3^2x_2x_3x_2)^2x_3 \\ &\quad (x_3x_2x_3^2x_2)^2x_3x_2)^2x_3(x_3x_2x_3^2x_2)^2x_3^2x_2 \\ &\quad (((x_3x_2x_3)^2x_2x_3)^2x_3x_2x_3x_2x_3)^2(x_3x_2x_3^2x_2)^2x_3 \\ &\quad (x_3x_2^{-1})^2x_2^{-1}x_1^{-1})^2 \end{aligned}$$

and gets  $m$  by

$$m = c_1 \cdot (f^7(c_2))^{-1} = x_3^{-2}x_2^2x_3x_1^2x_2^{-1}x_1^{-1}.$$

## 6 Conclusion

In comparison to the standard cryptosystems which are mostly based on number theory we explained two cryptosystems which use combinatorial group theory. The first cryptosystem in Section 4 is a one-time pad, which choice of the random sequence for encryption is not number-theoretic. At the moment it is costlier than the standard systems but it is another option for a one-time pad which is based on combinatorial group theory and not on number theory. The second cryptosystem in Section 5 is similar to the ElGamal cryptosystem (see [6]), which is easier to handle. The ElGamal cryptosystem is based on the discrete logarithm problem over a finite field. If this problem should eventually be solved we introduced here an alternative system, which is not based on number theory.

## References

1. G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger. *A Course in Mathematical Cryptography*. De Gruyter, 2015.
2. A. V. Borovik, A. G. Myasnikov, and V. Shpilrain. Measuring sets in infinite groups. *Contemporary Math. Amer. Math. Soc.* 298, pages 21–42, 2002.
3. T. Camps, V. große Rebel, and G. Rosenberger. *Einführung in die kombinatorische und die geometrische Gruppentheorie*. Berliner Studienreihe zur Mathematik Band 19. Heldermann Verlag, 2008.
4. V. Diekert, M. Kufleitner, and G. Rosenberger. *Diskrete Algebraische Methoden*. De Gruyter, 2013.
5. B. Eick, M. Kirschmer, and C. Leedham-Green. The constructive membership problem for discrete free subgroups of rank 2 of  $SL_2(\mathbb{R})$ . *LMS Journal of Computation and Mathematics*, 17 (1): pages 345–359, 2014.
6. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT-31: pages 469–473, 1985.
7. M. I. González Vasco and R. Steinwandt. *Group Theoretical Cryptography*. CRC Press, 2015.
8. J. Lehner. *Discontinuous Groups and Automorphic Functions*. Mathematical Surveys Number VIII. American Mathematical Society, Providence, Rhode Island, 1964.
9. R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Ergebnisse der Mathematik und ihre Grenzgebiete 89. Springer-Verlag, 1977.
10. W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory*. Pure and Applied Mathematics, A Series of Texts and Monographs Volume XIII. John Wiley & Sons, 1966.
11. Y. Matiyasevich. Solution of the Tenth Problem of Hilbert. *Mat. Lapok*, 21, pages 83–87, 1970.
12. A. I. S. Moldenhauer. *Cryptographic protocols based on inner product spaces and group theory with a special focus on the use of Nielsen transformations*. PhD thesis, University of Hamburg, 2016.
13. A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography*. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.
14. A. G. Myasnikov and V. Shpilrain. Automorphic orbits in free groups. *J. Algebra*, 269: pages 18–27, 2003.
15. J. J. Rotman. *An Introduction to the Theory of Groups*. Springer, 1995.
16. I. A. Stewart. Obtaining Nielsen Reduced Sets in Free Groups. *Technical Report Series*, 293, 1989.